

学校编码: 10384

分类号\_\_\_\_\_密级\_\_\_\_\_

学号: X2011230759

UDC\_\_\_\_\_

廈門大學

工 程 碩 士 學 位 論 文

安全电子商务网站的设计与实现

Design and Implementation of Secure E-commerce Website

帕尔哈提·伊德力斯

指 导 教 师: 吴清锋 副教授

专 业 名 称: 软 件 工 程

论文提交日期: 2014 年 3 月

论文答辩日期: 2014 年 4 月

学位授予日期: 年 月

指 导 教 师: \_\_\_\_\_

答辩委员会主席: \_\_\_\_\_

2014 年 月

## 厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为( )课题(组)的研究成果，获得( )课题(组)经费或实验室的资助，在( )实验室完成。(请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。)

声明人（签名）：

年 月 日

## 厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（        ） 1. 经厦门大学保密委员会审查核定的保密学位论文，  
于     年     月     日解密，解密后适用上述授权。

（    ☒    ） 2. 不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年    月    日

## 摘 要

随着电子信息技术的迅速普及和广泛应用,电子商务以其快捷、便利等优点越来越受到社会的认可。电子商务的出现不仅为互联网的发展提供了一个新的发展契机,也给社会经济注入了巨大能量。但电商以网络为主要载体的,大量的重要信息,比如说身份信息、交易信息都需要通过网络进行传输,因此,如何确保买卖双方信息,资金信息等安全问题成为首要问题。

为了解决上述问题,本文遵循商务网站建站的相关理论和技术,根据网络信息安全基本策略和方法,设计并实现一个安全的商务网站,以此作为对信息安全技术在商务网站建站中的应用的一个探路者。论文的主要内容包括:

1、对电商网站及其相关安全技术进行初步分析,特别是目前存在的一些主要问题。

2、分析了网站建设相关技术,重点从安全技术、数据加密、认证技术等进行了相关介绍,以及对开发技术进行简介。

3、根据商务网站建站需求,结合信息安全技术,进行了对系统总体和详细设计,比如:前台用户界面的设计,后台管理员界面的设计,后台数据库的设计,系统功能模块的设计和系统网络结构的设计等。

安全电子商务网站的建立,有助于进一步探讨商务网站的安全性问题。经测试,此网站结构层次合理,弥补现有商务网站一些安全性问题。

**关键字:** 多方计算; 信息安全; 数据库

## Abstract

With the rapid popularization of and wide application electronic information technology, e-commerce for its convenient advantages becomes more and more recognized by society. It not only provides a new opportunity for the development of Internet, also injects a huge amount of energy into the business world. But electronic commerce based on computer network, carrying a large number of important identity information, accounting information and transaction information needs to convey on the Internet. In this case, how to ensure that the buyer and the seller information and fund information security becomes a primary issue.

In order to solve these problems above, this dissertation uses theory and technology related to the establishment of the e-commerce site, according to basic strategy and method of network information security, designs and implements a secure e-commerce site, as to the information security technology in the application of e-commerce site a pathfinder. The main contents of this dissertation include:

1 Analysis the current situation of e-commerce and e-commerce security technology, find out the main problems.

2 Discuss the website building technologies, and technology in network security, data encryption, user authentication technology is introduced in aspects of the main electronic security technology; as well as a brief introduction of development technology.

3 According to the requirements of e-commerce site, combined the technology of information security, has carried on the overall and detailed design of system, such as: design of the front desk of the user interface, design of the background administrator interface, design of the backstage database, system function module design and the design of the system network structure, etc.

The establishment of this site helps to explore further security problems of e-commerce site. After testing, the website structure level is reasonable, and has make up some existing security problems of e-commerce site.

**Key words:** Multi-party Computation; Information Security; Database;

## 目 录

<b>第一章 绪论</b>	<b>1</b>
1.1 研究背景与意义	1
1.2 研究现状与进展	2
1.2.1 电子商务发展现状	2
1.2.2 电子商务安全技术发展现状及现存安全性问题	3
1.3 本文的主要研究工作	3
1.4 本文结构安排	4
<b>第二章 系统分析</b>	<b>5</b>
2.1 系统技术可行性分析	5
2.2 系统目标分析	6
2.3 系统功能需求分析	6
2.3.1 用户角色分析	6
2.3.2 前台子系统功能	7
2.3.3 后台子系统功能	7
2.3.4 用例图分析	8
2.4 系统性能分析	10
2.4.1 系统硬件分析	10
2.4.2 系统软件分析	11
2.5 小结	11
<b>第三章 建站技术概述</b>	<b>12</b>
3.1 商务站点简介及开发方法	12
3.2 开发技术	13
3.2.1 ASP 技术	14
3.2.2 .NET 技术	14
3.2.3 C#开发语言	15
3.2.4 ADO.NET 技术	15
3.3 小结	16

<b>第四章 系统设计</b>	<b>17</b>
<b>4.1 系统架构设计</b>	<b>17</b>
4.1.1 系统软件体系架构设计	17
4.1.2 系统网络拓扑结构设计	17
4.1.3 系统总体结构设计	18
4.1.4 系统的安全结构设计	19
<b>4.2 系统功能模块设计</b>	<b>19</b>
4.2.1 系统功能模块划分	19
4.2.2 管理员管理商品功能	20
4.2.3 商品交易实现过程	20
<b>4.3 系统业务流程设计</b>	<b>21</b>
4.3.1 用户购物流程	21
4.3.2 后台进入订单处理流程	22
<b>4.4 系统数据库设计</b>	<b>23</b>
4.4.1 Admin(管理员表)	24
4.4.2 ProductList(商品表)	24
4.4.3 Register(注册会员表)	25
4.4.4 ProductCar(购物车表)	25
<b>4.5 小结</b>	<b>26</b>
<b>第五章 系统实现</b>	<b>27</b>
<b>5.1 用户服务</b>	<b>27</b>
<b>5.2 显示商品</b>	<b>31</b>
<b>5.3 购物</b>	<b>33</b>
<b>5.4 系统后台管理</b>	<b>38</b>
<b>5.5 小结</b>	<b>40</b>
<b>第六章 总结与展望</b>	<b>41</b>
<b>6.1 总结</b>	<b>41</b>
<b>6.2 展望</b>	<b>41</b>
<b>参 考 文 献</b>	<b>43</b>

致 谢 .....	45
-----------	----

厦门大学博硕士论文摘要库



## Contents

<b>Chapter 1 Introduction .....</b>	<b>1</b>
<b>1.1 Research Background and Significance.....</b>	<b>1</b>
<b>1.2 Status Research .....</b>	<b>2</b>
1.2.1 E-commerce Development Status .....	2
1.2.2 E-commerce Security Technology Status and Issues.....	3
<b>1.3 Main Contents of this Dissertation.....</b>	<b>3</b>
<b>1.4 Organization Structure of this Dissertation .....</b>	<b>4</b>
<b>Chapter 2 System Analysis.....</b>	<b>5</b>
<b>2.1 Technical Feasibility Analysis .....</b>	<b>5</b>
<b>2.2 System Target Analysis .....</b>	<b>6</b>
<b>2.3 Functional Requirements Analysis .....</b>	<b>6</b>
2.3.1 User Roles .....	6
2.3.2 Main Functions .....	7
2.3.3 Background Requirements Analysis .....	7
2.3.4 Use Case Diagram Analysis .....	8
<b>2.4 System Performance Analysis .....</b>	<b>10</b>
2.4.1 System Hardware Analysis .....	10
2.4.2 System Software Analysis.....	11
<b>2.5 Summary.....</b>	<b>11</b>
<b>Chapter 3 Introduction to Related Technologies.....</b>	<b>12</b>
<b>3.1 Introduction of Commerce Website .....</b>	<b>12</b>
<b>3.2 Related Technologies.....</b>	<b>13</b>
3.2.1 ASP Overview .....	14
3.2.2 .NET Overview .....	14
3.2.3 C# Overview .....	15
3.2.4 ADO.NET Overview.....	15
<b>3.3 Summary.....</b>	<b>16</b>
<b>Chapter 4 System Design .....</b>	<b>17</b>
<b>4.1 System Architecture Design .....</b>	<b>17</b>

4.1.1 System Features Modular Design .....	17
4.1.2 Network Architecture .....	17
4.1.3 General Framework .....	18
4.1.4 System Security .....	19
<b>4.2 System Features Modular Design .....</b>	<b>19</b>
4.2.1 System Features Modular Design .....	19
4.2.2 Administrators Manage Process .....	20
4.2.3 Commodities Implementation Process .....	20
<b>4.3 Business Process Design .....</b>	<b>21</b>
4.3.1 Shopping Process .....	21
4.3.2 Background Order Processing .....	22
<b>4.4 System Database Design .....</b>	<b>23</b>
4.4.1 Admin(administrator table) .....	24
4.4.2 ProductList(merchandise table) .....	24
4.4.3 Register(Register Table) .....	25
4.4.4 ProductCar(shopping cart table) .....	25
<b>4.5 Summary .....</b>	<b>26</b>
<b>Chapter 5 System Implementation .....</b>	<b>27</b>
5.1 User Service .....	27
5.2 Product Display .....	31
5.3 Shopping .....	33
5.4 Background Management System .....	38
5.5 Summary .....	40
<b>Chapter 6 Conclusions and Prospects .....</b>	<b>41</b>
6.1 Conclusions .....	41
6.2 Prospects .....	41
<b>References .....</b>	<b>43</b>
<b>Acknowledgements .....</b>	<b>45</b>

## 第一章 绪论

计算机网络与通信技术一日千里、日新月异，每天都使用各式各样先进的通信设备发送和接收着丰富多彩的数据信息。可见，信息技术的迅速普及和应用已经深深地影响着我们生活的方方面面。在这信息爆炸的时代里，传统的商业活动、业务处理以及政府服务也已步入了信息网络的世界，一个开放性、无所不在的计算机网络 Internet。由此，产生了电子商务、在线业务办理、电子银行等信息类服务。近年来，商务网站的兴起，它们最大限度的利用信息技术和网络技术，使得传统的中小型企业摆脱了自身规模和地域的限制，从而使得自己在激烈的商务市场有一席之地。例如，我们熟知的淘宝的网购，无数小企业、个体成功的案例已经说明了这一点，同时崛起的电商包括：京东商城，当当，苏宁易购等，从早些年的网络购书到网络超市，网络商务提供了所有的商品信息。商务站点作为电子商务的基石，其作为一种崭新的商务运作模式，已经显现出巨大的商业价值，为我们的生活带来了巨大的便利，企业发展自己的电子商务，首先建立自己的电子商务网站已是势在必行。

商务信息数据作为一种社会资源，其本身也是一种财富，在不同利益的驱使下，使得网络上的用户变得异常复杂。在这样的复杂而又不安全网络环境下，建立可靠、安全、稳定的商务站点，保护商家和用户的网络数据通信和行为的信息安全、商业隐私数据，使用密码技术便是必不可少、行之有效的利器。人们熟知和常用的密码技术包括有：加密、数字签名、基于口令的用户认证等。

电子商务与电子商务站点平台的开放性、基于网络的信息共享性、动态性，使得商务站点安全问题异常突出。电子商务站点，其运作主要依托互联网平台完成交易，在这个过程中需要双方身份信息的验证，私人资金等敏感信息需要在网络上传输等，信息安全是交易双方最关心的问题。如何保证顺利的交易过程，信息的保密性、可控性、完整性、可用性，便是信息安全研究的主要问题。

### 1.1 研究背景与意义

从世界范围看，各国政府极为重视电子商务的开展，正如世界首富比尔·盖

茨所说：“21 世纪要么电子商务，要么无商可务！”。显然，电子商务作为世界发展的新趋势，不仅有着广泛的应用领域，十分诱人的发展前景，而且将逐步成为连接生产、流通和消费的极其重要的经济活动方式。

电子商务以其独特的优势解决了中小企业产业规模与地域间的限制，已经成为了新世纪经济增长的引擎。它的快速发展不仅对我们的生活带来了巨大的便利，而且对经济的发展也产生重大影响。面对世界电子商务发展的浪潮，我国许多企业也建立了自己的电子商务网站，搭建电子商务平台。然而，我国电子商务发展中的许多理论和实践问题尚未解决，特别是安全问题，给其发展带来了巨大的阻碍因素。因此，研究这些问题并采取相应的对策与措施来解决这些问题，将有助于电子商务在我国健康、迅速地发展。

## 1.2 研究现状与进展

### 1.2.1 电子商务发展现状

作为上个世纪人类最伟大的发明之一，上世纪 90 年代以来，Internet 在全球迅速普及并取得了迅猛的发展。在此前提下，电子商务网站应运而生。电子商务以卖方和买方为主体、以网上交易为结算手段、以 Internet 为载体，使买家与卖家更紧密联系在一起，更快满足客户的需求，同时也可以让企业在通过网络建立自己的品牌。

全球 B2B 电子商务交易一直占据主导地位，2002 年至今，呈现持续高速增长态势，2007 年全球 B2B 交易额达到 8.3 万亿美元，预计在未来几年将保持 40% 以上的增长率，到 2010 年 B2B 交易额将达到 26 万亿美元，比 2002 年增长 30 多倍。JP 摩根的高级分析师 Imran 卡恩发布了新年度报告，给予电子商务产业发展趋势给予了积极的预测。

该报告预测，全球电子商务收入将在 2010 年的基础上增长 18.9%，达到 6800 亿美元。美国网上零售商业则将增长 13.2%，至 1,870 亿美元。JP 摩根预计，2013 年全球电子商务市场规模将高达 9630 亿美元。

2007 年我国网上交易规模达到 17000 亿元。与 2006 年相比，增长了 25.5%。在综合类网站中，阿里巴巴已经占其中 7 成份额。2007 年我国电子商务网站收

入为 52.2 亿元，同比增长 33.5%。伴随着网络环境的好转以及企业电子商务化程度的提升，B2C 将会有有一个长足的发展，并成为未来网购的主流。

### 1.2.2 电子商务安全技术发展现状及现存安全性问题

建站技术始于上世界 80 年代，主要是基于 HTML 标记性语言，后来发展到集成各类功能的框架结构，随着面向对象语言的广泛应用，动态网站的崛起，建立交互性网站的技术主流的主要包括了：微软的 ASP.NET，基于 Java 语言的 JSP 的，以及开源的 PHP。当前，在互联网跑着的网站主要是基于开源的 PHP，首先是开源的，免费的，交互性，架构都是非常成熟的 LAMP 架构，主要是 Linux（操作系统）+ Apache（Web-Server）+MySQL（数据库）+PHP（业务逻辑语言）。

20 世纪 70 年代，美国发布的共用数据加密标准 (DES, Data Encryption Standard) 和公钥密码体制 (PKC, Public key Cryptosystem) 的诞生，标志着信息安全密码学正式进入的飞速发展的时期 (W. Daffier et al, 1976)。基于公钥加密算法的数字签名、身份认证和数字证书等迅速普及和广泛应用，密码学技术不再是只掌握在少数人手中的知识，仅局限于军事、政治外交等国家应用领域，它已经逐步渗透到我们日常生活各个方面，如在线商品交易、电子支付、社交等活动。

如何建立安全的电子商务网站，安全的网络交易协议的设计是电子商务中主要研究课题之一。随着建站技术的日益成熟和信息安全不断引入到建站之中，为网络用户和商家提供了安全保障。建站的目的已经不仅仅是建立商家和客户间的交易桥梁，同时商家可以进行有效的数据收集，抵制不安全的用户行为，挖掘新的用户喜好，更好的迎合用户的需求，发展和壮大自己的产业等。在传统的商务广泛的应用数据挖掘，帮助商家制定营销策略、计划来支持这些商务活动。

## 1.3 本文的主要研究工作

通过查阅和学习电子商务站点建站技术与信息安全的基础知识，分析和总结了前人对建站与互联网安全的研究工作和主要贡献结果。

(1) 本文通过对现今电子商务网站的调研，比如淘宝网，卓越网等等，致力于研究电子商务建站技术，分析其中可能存在的安全漏洞与安全威胁根据目前

发展的瓶颈，探讨如何结合信息安全在实践建站中的应用。

(2) 遵循软件工程的设计思想，分析其系统总体需求，功能性需求，安全需求等，并且进行了简单的电子商务站点的整体设计过程，以及在电子商务最常使用的交易平台进行有效的身份认证。

(3) 建立简单的商务站点，以此实践本文提出的安全策略。

## 1.4 本文结构安排

第一章：绪论。主要是概述研究背景和意义，以及当前互联网技术的发展，信息网络通信技术如何影响和改变着我们的日常生活，并分析电子商务网站的发展现状及安全现状。

第二章：系统分析。从系统应用背景、技术可行性、目标、功能和安全风险等角度对本系统进行分析。

第三章：建站技术概述。主要从开发方法、信息安全技术和开发技术等方面扼要地介绍了系统研发所涉及的若干关键技术。

第四章：系统设计。在概述系统设计原则的基础上，从头系统架构、功能模块、业务流程、数据库和安全等对系统进行了设计。

第五章：系统实现。通过代码和界面截图等形式展现了系统的若干核心功能模块，如：用户服务、商品现实、后台管理等。

第六章：总结与展望。在总结论文工作和系统特色的基础上，对下一步的工作进行了展望。

## 第二章 系统分析

随着因特网的发展，网上购物将逐步演变为 21 世纪的主要贸易方式之一。网上购物是一种具有交互功能的商业信息系统，伴随网络技术的发展，电子商务也成为了人们日益关注的焦点所在。各个企业都认识到建立一个电子商务平台，可以大大拓宽自身营销渠道，同时还可以对品牌形象的提升带来重要战略意义。

### 2.1 系统技术可行性分析

现如今，计算机网络已经遍布世界各个角落，为了方便购物者可以随时随地使用本系统，因此本系统决定采用 B/S 结构。B/S 架构软件的优势与劣势体现在以下几个方面：

（1）维护和升级简单。其中开发、维护等工作都集中在服务器，因此对网络进行升级时，更新服务器就可以，这大大减轻了维护与升级的成本。

（2）性能有保证

在任何时间、任何地点、任何系统，只要可以使用浏览器上网，就可以使用 B/S 系统的终端。

（3）系统的开发

C/S 结构是建立在中间件产品基础之上的，要求应用开发者自己去处理事务管理、消息队列、数据的复制和同步、通信安全等系统级的问题。这对应用开发者提出了较高的要求。管理软件是企业服务的，企业选用管理软件不仅要从技术上考虑，还要从商业运用方面来考虑，对于集团来讲，B/S 结构可以方便的对软件项目进行控制，但是 C/S 结构不同，随着软件应用范围扩大，后期所需要的投资会接连不断。

在硬件设备的投资方面，C/S 结构和 B/S 结构也不一样。应用范围增大，系统负担上升时，C/S 结构就需要升级服务器设备，很有可能原有服务器就被放弃不用，由于 C/S 软件的结构性造成这种软件的服务器端要被部署在一台服务器上；而 B/S 结构不同，伴随着服务器负担增加，只需要增加服务器个数并在各服务器之间保持负载均衡就可以。

其次，伴随软件的扩张，对人才的需求很有可能变成制约企业扩张的瓶颈。对专业维护人才的需求会是企业面临的挑战。

## 2.2 系统目标分析

在 Internet 技术深入人心的今天，电子商务作为一种新兴的商务模式，为世界经济提出了一个全新的概念，使得人类生活方式发生了重大的变革。

本文所研究的网上购物系统，旨在通过电子商务来使得人们购物变得更方便，更安全。系统分为前台后台管理两个部分。前台管理面向用户的操作界面，提供浏览、查询功能。用户可以进行浏览、查询、订购等操作；后台提供给管理员进行操作的，包括：商品、用户管理等功能。这种结构可以将管理员从手工操作中解脱，并大大提高了效率。

## 2.3 系统功能需求分析

### 2.3.1 用户角色分析

一个商务网站，一般由四类人员参与，他们包括：游客用户，注册用户，管理员，系统管理员等。下面对各类人员进行角色分析：

(1) 游客用户 (Guest)：该类人员的权限为最低级（第四级），只能用于页面商品浏览，页面商品搜索等操作，不涉及购物车，个人账户管理方面的操作。

(2) 注册用户 (Register)：该类人员的权限（统为第三级，然后将其细分）按照其积分的不同予以一定的区分，简单的分类比如 Vip1 到 Vip7，每级逐级开放特权，比如优惠券，抵价券，积分换商品之类。要获得高等级的权限，必须实名认证（经过实名制审核，且与公安部网站联网认证），邮箱，手机认证等等；网站相关人员必须对该类会员进行实质性的考核，达到要求之后，予以认定其权限。该类人员是商务网站得以生存的关键。

(3) 管理员 (Webmaster)：该类人员具有较高权限（第二级），该类人员分：网站日常运营维护人员；网站商品管理人员；用户和评论管理人员；客服等。其职责是负责网站的正常运营和用户诉求的及时处理等。



Degree papers are in the "[Xiamen University Electronic Theses and Dissertations Database](#)". Full texts are available in the following ways:

1. If your library is a CALIS member libraries, please log on <http://etd.calis.edu.cn/> and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to [etd@xmu.edu.cn](mailto:etd@xmu.edu.cn) for delivery details.

厦门大学博硕士论文摘要库